Security & Chip Card ICs

SLE 66CX320P

16-Bit Security Controller
with Memory Management Unit
in 0.25 µm CMOS Technology
64 Kbyte ROM, 3 Kbytes RAM, 32 Kbyte EEPROM
1100-Bit Advanced Crypto Engine and 64-Bit DES accelerator

Preliminary Short Product Information 07.99

SLE 66CX320P Preliminary Short Product Information	
This document contains preliminary information on a new product under development. Details are subject to change without notice. **Revision History: Current Version 07.99**	
Previous Releases:	
Page	Subjects (changes since last revision)

Important: Further information is confidential and on request. Please contact:
Infineon Technologies AG in Munich, Germany,
Security & Chip Card ICs,
Fax +49 89 234-28925

Published by Infineon Technologies AG i.Gr., CC System Engineering Group
St.-Martin-Strasse, D-81541 München

Attention please!

The information herein is given to describe certain components and shall not be considered as warranted characteristics.

Terms of delivery and rights to technical change reserved.

We hereby disclaim any and all warranties, including but not limited to warranties of non-infringement, regarding circuits, descriptions and charts stated herein.

Infineon Technologies is an approved CECC manufacturer.

Information

For further information on technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies Office in Germany or our Infineon Technologies Representatives world-wide (see address list).

Warnings

Due to technical requirements components may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies Office.

Infineon Technologies Components may only be used in life-support devices or systems with the express written approval of Infineon Technologies, if a failure of such components can reasonably be expected to cause the failure of that life-support device or system, or to affect the safety or effectiveness of that device or system. Life support devices or systems are intended to be implanted in the human body, or to support and/or maintain and sustain and/or protect human life. If they fail, it is reasonable to assume that the health of the user or other persons may be endangered.

16-Bit Security Controller with MMU in 0.25µm CMOS Technologie 64 Kbyte ROM, 3 Kbytes RAM, 32 Kbyte EEPROM, 1100-Bit Advanced Crypto Engine and 64-Bit DES accelerator

Features

- 16-bit microcomputer in 0.25 µm CMOS technology
- Instruction set opcode compatible with standard SAB 8051 processor
- Enhanced 16-bit arithmetic
- Additional powerful instructions optimized for chip card applications
- Dedicated, non-standard architecture with **execution time six times faster** than standard SAB 8051 processor at same clock
- **63 Kbytes User ROM** for application programs
- 1 Kbyte reserved ROM for Resource Management System (RMS) with intelligent EEPROM write/erase routines
- **32 Kbytes EEPROM**
- **2 Kbyte** XRAM, 256 Bytes IRAM, 700 Bytes Crypto RAM
- **Memory Management Unit**
- **DES and EC2 accelerator (GF 2^n)**
- **Advanced Crypto Engine**
- CRC Module
- Interrupt Module
- **PLL**
- 16-bit Autoreload Timer
- Power saving sleep mode
- **Ext. clock freq. 1 to 7.5 MHz for int. clock ≤ 15 MHz**
- **UART for handling serial interface** in accordance with ISO 7816 **supporting transmission protocols T=1 and T=0**
- I/O routines realized in software executable
- Supply voltage range: 2.7 V to 5.5 V
- Current consumption < 10 mA at 15 MHz internal and 5.5 V
- Temperature range: -25 to +70°C
- ESD protection larger than 4 kV

EEPROM

- Reading, erasing and writing byte by byte
- Flexible page mode for 1 to 64 bytes write/erase operation
- 32 bytes security area
- Write time < 4.5 ms
- Programming time independent of clock frequency
- **Minimum of 700.000 write/erase cycles at 25°C**
- Data retention for a minimum of 10 years
- EEPROM programming voltage generated on chip

MMU

- Addressable memory up to 1 MByte
- Separates OS (system) and application (user)
- System routines called by traps
- OS can restrict access to peripherals in application mode
- Code execution from XRAM possible

Security Features

- Low and high voltage sensors
- Low-frequency sensor
- High-frequency filter
- True Random Number Generator
- Internal power-on-reset
- 16 bytes security PROM, hardware protected
- Unique chip identification number for each chip
- Security optimized layout
- Additional security features

Support

- HW-& SW-Tools (Emulator, ROM Monitor, Card Emulator, Simulator)
- Application notes

Features (cont'd)

Performance Advanced Crypto Engine

Operation	Modulus	Exponent	Calculation Time at 5 MHz	Calcul. Time at 15 MHz
Modular Exponentiation	160 bit	160 bit	20 ms	7 ms
Modular Exponentiation	256 bit	256 bit	35 ms	12 ms
Modular Exponentiation	512 bit	512 bit	110 ms	37 ms
Modular Exponentiation RSA Encrypt / RSA Signature Verify	1024 bit	16 bit	20 ms	7 ms
Modular Exponentiation RSA Decrypt / RSA Signature Generate	1024 bit	1024 bit	820 ms	273 ms
Modular Exponentiation using CRT RSA Decrypt / RSA Signature Generate	eq.1024 bit	eq.1024 bit	250 ms	83 ms
DSA Signature Generate	512 bit	160 bit	145 ms	48 ms
DSA Signature Verify	512 bit	160 bit	130 ms	43 ms
DSA Signature Generate	1024 bit	160 bit	290 ms	97 ms
DSA Signature Verify	1024 bit	160 bit	360 ms	120 ms
Elliptic Curves EC-GDSA Sign. Generate	160 bit	160 bit	260 ms	87 ms
Elliptic Curves EC-GDSA Sign. Verify.	160 bit	160 bit	550 ms	183 ms

Performance DES accelerator

Operation	Data block length	No. of clock cycles to en-/ decrypt an 8 byte block	Encryption time for an 8 byte block incl. key loading + data transfer	
			5 MHz	15 MHz
56-bit Single DES Encryption	64 bit	32	20 µs	7 µs
112-bit Triple DES Encryption	64 bit	98	37 µs	12 µs

Ordering Information

Type	Package[1]	Voltage Range	Temperature Range	Frequency Range (ext. clock frequency)
SLE 66CX320P M4	M4	2.7 V - 5.5 V	– 25°C to + 70°C	1 MHz - 5 MHz
SLE 66CX320P C	C			
SLE 66CX320P-T85 M4	M4	2.7 V - 5.5 V	– 25°C to + 85°C	1 MHz - 5 MHz
SLE 66CX320P-T85 C	C			
SLE 66CX320P-F7 M4	M4	2.7 V - 5.5 V	– 25°C to + 70°C	1 MHz – 7.5 MHz
SLE 66CX320P-F7 C	C			

Pin Configuration

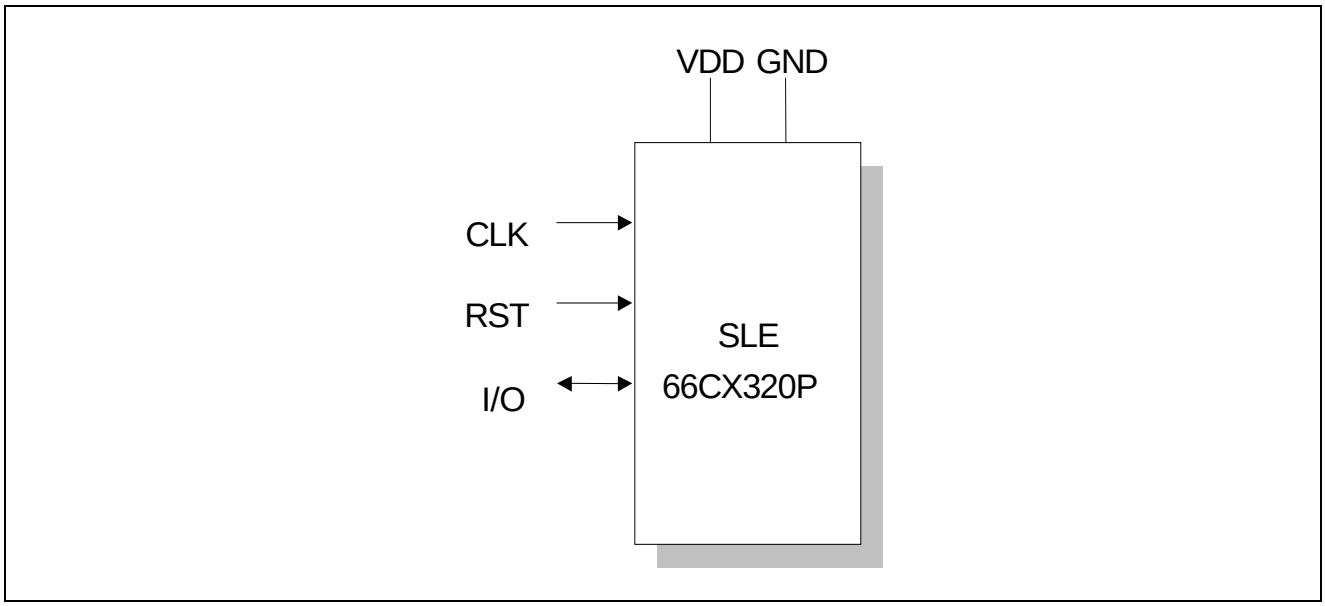

Figure 1 Pin Configuration

Pin Definitions and Functions

Symbol	Function
VCC	Operating voltage
RST	Reset input
CLK	Processor clock input
GND	Ground
I/O	Bi-directional data port

[1] available as wire-bonded module (M4) for embedding in plastic cards or as die (C) for customer packaging

General Description

SLE 66CX320P is the first product of Infineon Technologies high end security controller family in advanced 0.25 µm CMOS technology. The CPU provides the high efficiency of the SAB 8051 instruction set extended by additional powerful instructions together with enhanced performance, memory sizes and security features. The internal clock frequency can be adjusted up to 15 MHz independent of the clock rate of the terminal with the help of the PLL.

The controller IC offers 63 Kbyte of User-ROM, 256 bytes internal RAM, 2048 bytes XRAM and 32 Kbytes EEPROM. The Memory Management Unit allows a secure separation of the operating system and the applications. Furthermore the MMU makes a secure downloading of applications possible after the personalization of a card. These new features suit the requirements of the next generation of multi application operating systems. For code compatibility to the SLE 66CxxS family, a transparent mode for the MMU is established which allows to keep the memory mapping of the SLE 66CxxS products.

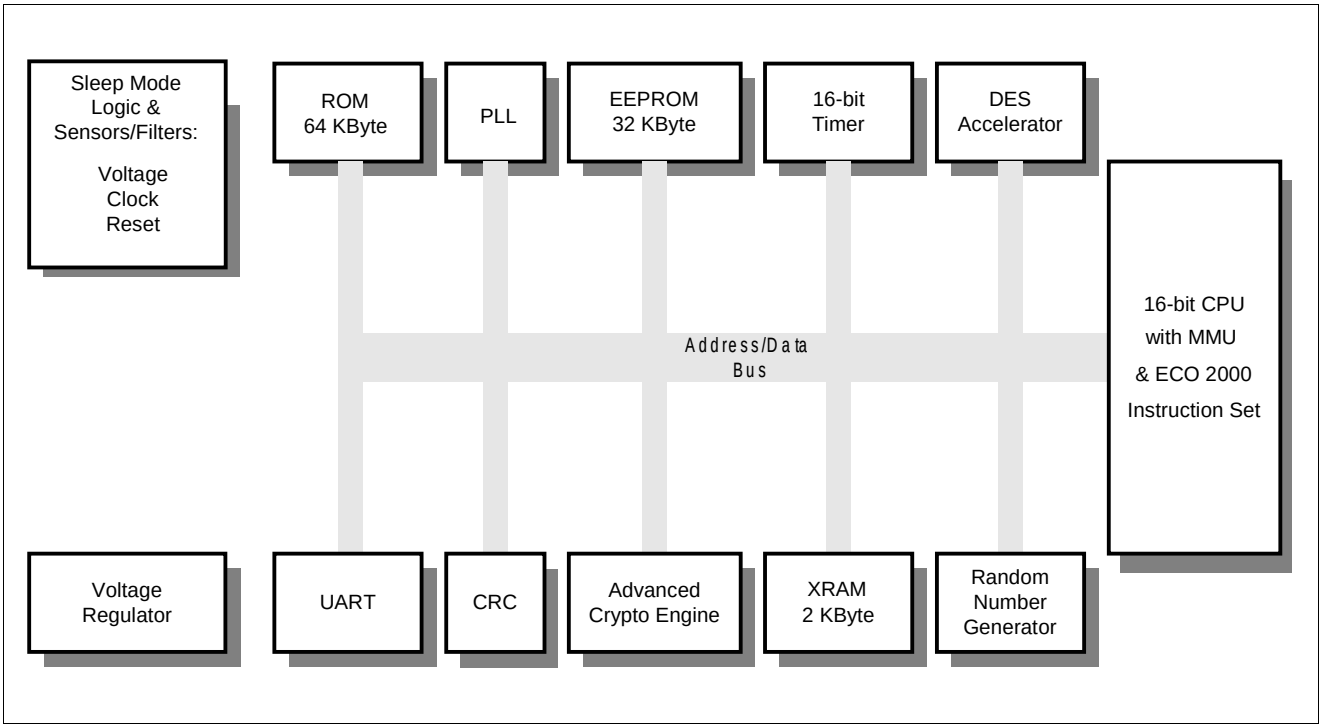

Figure 2 Block Diagram SLE 66CX320P

The CRC module allows the easy generation of checksums according to ISO 3309 (16-Bit-CRC). To minimize the overall power consumption, the chip card controller IC offers a sleep mode. The UART supports the half-duplex transmission protocols T=0 and T=1 according to ISO 7816-3. All relevant transmission parameters can be adjusted by software, as e.g. the clock division factor, direct/inverse convention and the number of stop bits. Additionally, the I/O port can be driven by communication routines realized in software.

The Advanced Crypto Engine is equipped with its own RAM of 700 bytes and supports all of today known public-key algorithms based on large integer modular arithmetic. It allows fast and efficient calculation of e.g. RSA operations with key lengths up to 2048 bit.

The DES accelerator consists of two modules. The DES module supports symmetrical crypto algorithms according to the Data Encryption Standard in the Electronic Code Book Mode. The EC2 module accelerates the multiplication in GF(2^n) and therefore the operations for elliptic curve cryptography.

The random number generator (RNG) is able to supply the CPU with true random numbers on all conditions.

As an important measure, the chip provides a new and enhanced level of on-chip security features.

In conclusion, the SLE 66CX320P fulfills the requirements of today's chip card applications, as Banking, GSM, Pay TV, security access and digital signature and offers a powerful platform for future multi application cards. The SLE 66CX320P integrates outstanding memory sizes, additional peripherals in combination with enhanced performance and optimized power consumption on a minimized die size. Therefore, the SLE 66CX320P offers the basis for a generation of new chip card applications.